

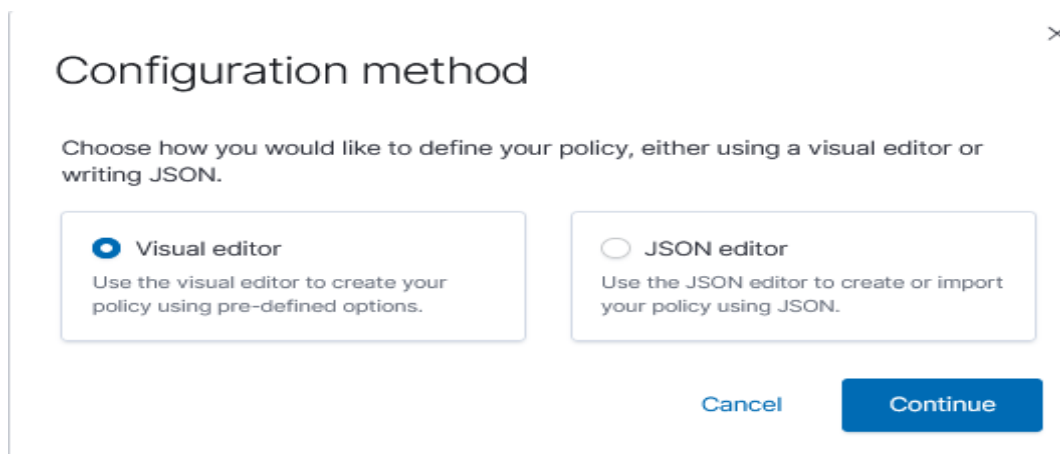
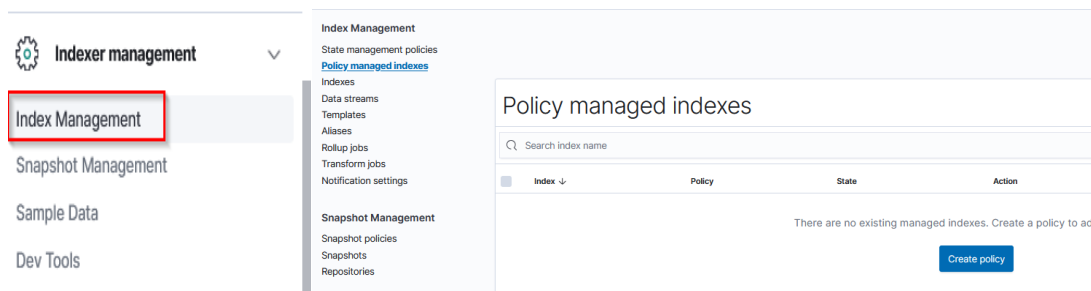
Création d'une politique de rétention

Dans cette documentation nous verrons comment créer une politique de rétention des logs.

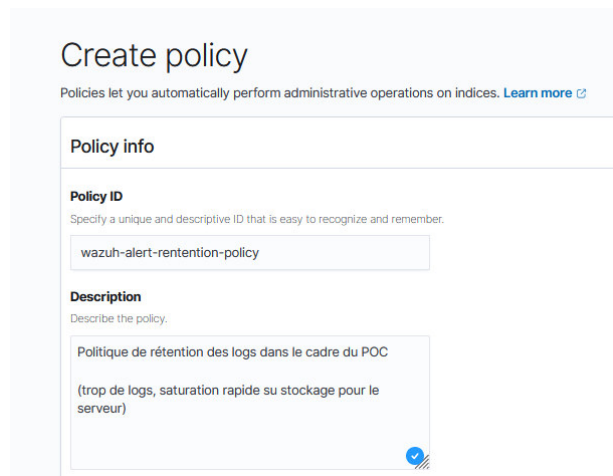
<https://documentation.wazuh.com/current/user-manual/wazuh-indexer-cluster/index-lifecycle-management.html>

Utilisation de l'éditeur visuel

Cliquez sur le menu en haut à gauche ☰, allez dans **Gestion de l'indexeur**, et sélectionnez **Gestion des index**. Choisissez **Politiques de gestion d'état** et cliquez sur **Créer une politique**. Sélectionnez **Éditeur visuel** et cliquez sur **Continuer** :



Entrez un **ID de politique** unique dans la section **Policy ID**. Par exemple, `wazuh-alert-retention-policy`. Vous pouvez éventuellement décrire la politique dans le champ **Description** :



Create policy

Policies let you automatically perform administrative operations on indices. [Learn more](#)

Policy info

Policy ID
Specify a unique and descriptive ID that is easy to recognize and remember.

wazuh-alert-retention-policy

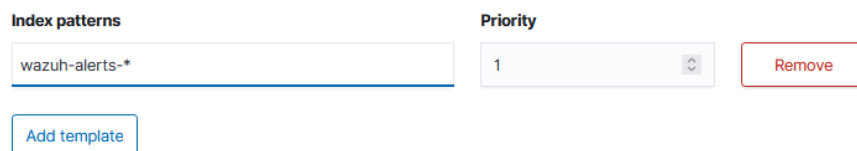
Description
Describe the policy.

Politique de rétention des logs dans le cadre du POC
(trop de logs, saturation rapide du stockage pour le serveur)

Cliquez sur **Ajouter un modèle** sous **Modèles ISM** et entrez un modèle d'index tel que `wazuh-alerts-*` pour appliquer automatiquement cette politique aux futurs index d'alertes. La priorité est définie par défaut et peut être modifiée. L'index avec la valeur de priorité la plus élevée est traité en premier :

ISM templates – optional

Specify ISM template patterns that match the index to apply the policy. [Learn more](#)



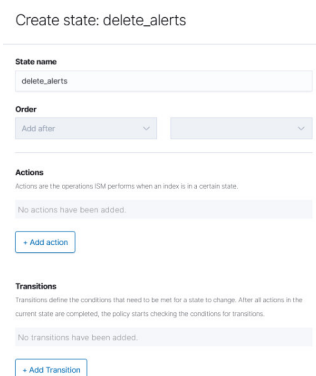
Index patterns	Priority	
wazuh-alerts-*	1	Remove

[Add template](#)

Le * permet de sélectionner tout les types d'alertes.

- [Add template](#)

Cliquez sur **Create state** pour créer un état de suppression d'index. Entrez un nom tel que `delete_alerts` :



Create state: delete_alerts

State name
delete_alerts

Order
Add after

Actions
Actions are the operations that the system performs when an index is in a certain state.
No actions have been added.
[Add action](#)

Transitions
Transitions define the conditions that need to be met for a state to change. After all actions in the current state are completed, the system starts checking the conditions for transitions.
No transitions have been added.
[Add Transition](#)

Cliquez sur **Ajouter une action** et sélectionnez **Supprimer** dans le **Type d'action**. Cliquez sur **Ajouter une action**. Puis cliquez sur **Enregistrer l'état** :

State: delete_alerts

Add action
Actions are the operations ISM performs when an index is in a certain state. [Learn more](#)

Action type
Select the action you want to add to this state.

Delete

- Cliquer sur Add action
- Save State

Cliquez à nouveau sur **Create state** pour créer un état initial. Entrez un nom, tel que `initial` :

States (1)
You can think of policies as state machines. "Actions" are the operations ISM performs when "Transitions" define when to move from one state to another. [Learn more](#)

Initial state: delete_alerts

> delete_alerts Initial state Actions 1

Add state

Choisissez **Add before** dans l'onglet **Order** et sélectionnez **delete_alerts** :

Create state: initial

State name

initial

Order

Add before delete_alerts

Cliquez sur **Add Transition** et sélectionnez **delete_alerts** comme **État de destination**, sélectionnez **Âge minimum de l'index** dans **Condition**. Saisissez la valeur de rétention, dans notre cas, ce sera 2jours

State: initial

Add transition
Transitions define the conditions that need to be met for a state to change. After all actions in the current state are completed, the policy starts checking the conditions for transitions. [Learn more](#)

Destination state
If entering a state that does not exist yet, then you must create it before creating the policy.

delete_alerts

Condition
Specify the condition needed to be met to transition to the destination state.

Minimum Index Age

Minimum index age
The minimum age required to transition to the next state.

2d

- La politique a bien été créée, maintenant il faut attendre 2 jours pour voir si celle-ci fonctionne bien.

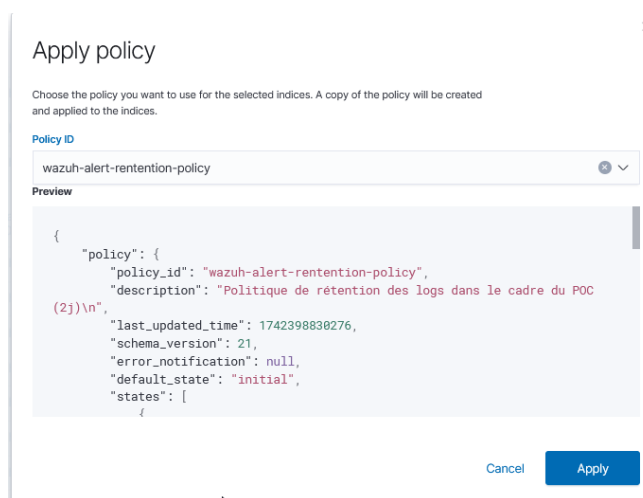
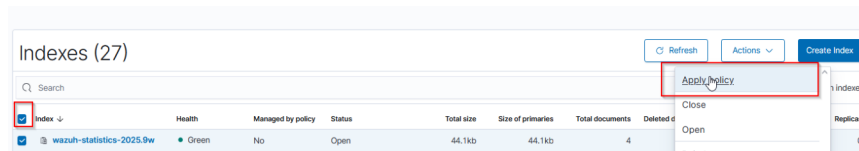


Appliquer la politique aux alertes

Cliquez sur le menu en haut à gauche ≡, allez dans Gestion de l'indexeur, et choisissez Gestion des index. Sélectionnez Indices.

Sélectionnez l'index ou les indices auxquels vous souhaitez attacher la politique.

Cliquez sur Actions > Appliquer la politique.



- Apply

JSON de la politique :

```
{ "policy": { "policy_id": "wazuh-alert-rentention-policy", "description": "Politique de rétention des logs dans le cadre du POC (2j)\n", "last_updated_time": 1742398830276, "schema_version": 21, "error_notification": null, "default_state": "initial", "states": [ { "name": "initial", "actions": [], "transitions": [ { "state_name": "delete_alerts", "conditions": { "min_index_age": "2d" } } ] }, { "name": "delete_alerts", "actions": [ { "retry": { "count": 3, "backoff": "exponential", "delay": "1m" } }, { "delete": {} } ], "transitions": [] }, "ism_template": [ { "index_patterns": [ "wazuh-alerts-*" ], "priority": 1, "last_updated_time": 1742398007136 } ] }
```

Détails de la politique :

Nom de la politique : `wazuh-alert-rentention-policy`

Description : Politique de rétention des logs pour le POC (2 jours)

Transitions d'état :

- État initial (`initial`) : Dans cet état, aucune action n'est effectuée. Cependant, il y a une transition vers l'état `delete_alerts` lorsque les conditions sont remplies.
- Condition de transition : La condition pour passer à l'état `delete_alerts` est un âge d'index minimum de 2 jours (indiqué par `"min_index_age": "2d"`). Cela signifie que les indices qui ont plus de 2 jours seront considérés pour suppression.

État de suppression des alertes (`delete_alerts`) :

- Action : Une action de suppression est définie dans cet état, ce qui implique que les indices seront supprimés.
- Tentatives de suppression : Si la suppression échoue, l'action tentera de se répéter 3 fois avec un délai de 1 minute entre chaque tentative (backoff exponentiel).

Template ISM appliqué : La politique est appliquée aux indices ayant le modèle `wazuh-alerts-*`, ce qui signifie que tous les indices correspondant à ce modèle seront gérés par cette politique.